EPA Classification No.: 2100.5	CIO Approval Date: 4/7/06
CIO Transmittal No.: 06-009	Review Date: 4/09

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

SYSTEM LIFE CYCLE MANAGEMENT POLICY

1. PURPOSE

This System Life Cycle Management (SLCM) Policy promotes effective and efficient solution(s) for designing and operating information systems, through a process of progressive steps to ensure proper management review and approval, as well as integration with the Agency's IT security, Enterprise Architecture (EA) and IT Investment Management processes, while allowing flexibility to accommodate varying developmental approaches.

2. SCOPE AND APPLICABILITY

This policy applies to:

1. Information systems developed, enhanced, or maintained by or for EPA; this includes Commercial Off-The-Shelf Software (COTS), Government Off-The-Shelf acquisitions (GOTS) and E-Government projects utilized directly within the EPA network. This also includes applications and general support systems, whether internal or contractual, IT infrastructure, programmatic and administrative systems and projects. This Policy exempts small desktop applications.

2. Anyone or any group who develops, supports, is responsible for, and/or operates an information system to collect or maintain information on behalf of EPA.

3. AUDIENCE

The audience for this policy includes the Chief Information Officer (CIO), Chief Financial Officer (CFO), Senior Information Officials (SIO), Information Management Officers (IMO), project managers of IT systems, and any person involved in the development and management of EPA IT systems and applications.

4. BACKGROUND

EPA Classification No.: 2100.5	CIO Approval Date: 4/7/06
CIO Transmittal No.: 06-009	Review Date: 4/09

Information resources increasingly consume an ever larger share of the Federal Budget, and new laws and regulations, in particular the Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002, and Office of Management and Budget Circulars A-11 and A-130, require EPA to ensure its System Life Cycle Management Policy is comprehensive and up-to-date.

5. AUTHORITIES

1. Chief Financial Officers Act of 1990

2. Clinger-Cohen Act of 1996, formerly the Information Technology Management Reform Act

3. Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995

4. Federal Information Security Management Act of 2002 (FISMA)

5. Government Paperwork Elimination Act (GPEA) of 1998

6. Privacy Act of 1974, as amended

7. High Performance Computing Act of 1991

8. Executive Order No. 13011 of July 16, 1996, *Federal Information Technology*

9. Presidential Decision Directive 63 (PDD 63), *Protecting America's Critical Infrastructures,* May 1998

10. Joint Federal Management Improvement Program, "Framework for Federal Financial Management Systems," April 2004

11. Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998

6. POLICY

A. *Transition*

In order to provide for an orderly transition, projects do not need to re-document phases completed under the Interim System Life Cycle Management Policy. Projects must meet the Policy requirements established as of the stage/phase that the project is in when this Policy is issued. Only work performed from the approval date of this Policy is expected to conform to all the requirements of this SLCM Policy.

B. *General*

1. The EPA System Life Cycle (SLC) is an ordered series of activities that define, develop, implement, operate/maintain, and terminate an information system.

2. Information security considerations, activities and documentation are performed at each phase of the SLC in accordance with Agency policies and applicable Federal statutes, regulations, Executive Orders, OMB Circulars and other applicable guidance.

3. IT Investment Management, specifically Capital Planning and Investment Control (CPIC), Enterprise Architecture (EA), privacy, and records management considerations, activities and documentation are performed based on applicable Federal and Agency requirements (see VI. Authorities and Appendix 1) as the information system proceeds through its life cycle. Associated funding actions must follow the IT Cost Accounting structure established and maintained by the Office of Chief Financial Officer.

4. The life cycle phases needed to deliver a desired information system must be identified, planned for and executed based on the specific requirements of the business unit. The order of implementing the phases and the level of detail required to complete them will vary on a system-by-system basis. For each project, the key to effectively using the SLCM methodology lies in adapting the life cycle phases and deliverables to best suit the needs and characteristics of the project. Such adaptation must be documented and, if appropriate, approved through the waiver process.

5. All information system development or acquisition must use recognized project management and support activities, processes and techniques. The SLCM Procedure supporting this Policy describes the appropriate activities, processes and techniques.

6. Whenever possible EPA information system requirements should be met by using COTS or GOTS software products. Agency business processes should be modified to match the functional features of the products to the extent practicable.

7. Developing systems in a rigorous manner reduces and manages risk. To minimize the risk of failed systems, all Major Applications and General Support Systems, and systems considered to be Major Investments in the CPIC process, will use a methodology consistent with EPA technical standards. Sound methodology promotes reliable and valid development practices, and on-time and on-budget delivery consistent with Earned Value Management (EVM).

C. ***System Life Cycle Phases, Security and Cost Accounting*** 1. A system life cycle at EPA consists of five phases: Definition, Acquisition/Development, Implementation, Operations and Maintenance, and Termination.

System documentation must be reviewed, revised and updated as needed based on requirements throughout the system's life cycle.

2. The **Definition Phase** requires defining an EPA business need. It documents the purpose, scope and requirements of the proposed information system. The solutions are reviewed and approved through applicable EA, CPIC, IT security, and cost accounting procedures. The compilation of documents identified as a Systems Management Plan (SMP) begins during this phase.

3. The **Acquisition/Development Phase** uses information from the Definition Phase to design, develop and/or acquire the information system that meets the EPA business need. During this phase the security requirements of the system are refined and updated. Contingency plans or continuity of operations plans (COOP) are developed and CPIC requirements are reported.

4. The **Implementation Phase** establishes the system in a production environment. Data

are converted as needed, and sample testing is conducted to verify the system. Also security certifications must be conducted and CPIC requirements must be reported. Prior to beginning the next phase of operations, the system must have a written authorization to operate and proceed.

5. The **Operation and Maintenance Phase** includes activities for the system's ongoing functions and maintenance. This Phase requires periodic risk assessments, testing, re-certification and reauthorization, CPIC, IT security, and cost accounting reviews, and an EA annual review.

6. The **Termination Phase** ends the operation of the system in a planned, secure, orderly manner, including archiving system components and data or incorporating them into other systems as required, and securely disposing of hardware and software as appropriate.

7. The procedures, standards and guidance supporting this Policy identify the specific activities and documents required during each phase of the life cycle.

D. ***Management Review and Approval***

1. All EPA information systems must have a documented, designated System Sponsor, System Owner, System Manager and Project Manager with unique system management, review, and approval functions to support the system life cycle management process. Please see Section 8. Roles and Responsibilities.

2. EPA managers responsible for a system must review and approve the system's decision documents at each SLCM phase, and document the reviews and approvals in the system's decision documents and SMP. All information systems must have written management approval before being deployed.

3. Prior to incremental funding of each stage of SLCM, managers must approve appropriate documentation. The Quality and Information Council (QIC) approves major investments in information systems through the CPIC process.

4. Advancement from one SLCM phase to the next may require an Enterprise Architecture or an IT Investment Management review. These reviews are designated Agency-level control gates (see Section 9. "Definitions") and management must ensure they take place. When a control gate review is required, management must not advance a system without documented, written approval resulting from that review. Additionally, management must ensure that all calendar driven checkpoints (see Section 9. "Definitions") occur. These checkpoints support, and coincide with, CPIC and Security data calls.

5. When a system is "owned" by more than one program or Agency, the affected organizations form a steering committee comprised of senior officials with authority to address cross program issues, including funding and program requirements.

E. ***System Classification***

The classification (see Section 9. Definitions) of a system determines the life cycle activities for each phase. This includes the necessary system documentation, level of detail, and the degree of adaptability to suit the needs and characteristics of the project. This Policy excludes small desktop applications.

The SLCM Procedure addresses specific requirements for systems based on their classification.

F. *System Life Cycle Management*

1. The System Manager and Project Manager are responsible for ensuring that the system advances in an orderly fashion through the SLCM phases and, while not mandatory, system products should take into account EPA's Information Quality Guidelines.

2. Activities must be planned for each SLCM phase. Requirements are the same for general support/infrastructure systems and programmatic/administrative systems. The level of detail of each section however, should be consistent with the size of the system. System Managers are responsible for tailoring their SLCM, including obtaining appropriate waivers, to meet the requirements of their system.

3. Although all phases must be completed and documented, they do not need to occur in a linear fashion and non-linear development does not require a waiver.

4. System life cycle management requires documentation. Documenting each major step/element and the project's Solution Architecture will help ensure sound life cycle management, Enterprise Architecture compliance, and alignment with IT investment management processes. A System Management Plan (SMP) refers to SLC documents as a whole. It includes the information that the System Owner approves at appropriate control gates, checkpoints and review points (as applicable) in the SLCM phases. Compiling SMP documents begins in the Definition Phase. The SMP receives updates and supplements continuously throughout the system's life cycle. The SLCM Procedure defines the basic contents of a SMP.

5. A "Solution Architecture" is developed, maintained, and certified as compliant with the Agency Enterprise Architecture at appropriate checkpoints throughout the project's life cycle.

6. An approved Security Plan is required for all operational components of a system. The Security Plan also must take into account those components under development.

7. The design aspects of the SLC may require tailoring for COTS or GOTS acquisitions. Interactions with other systems or modifications to the COTS or GOTS product require appropriate documentation. The SLCM Procedure describes potential ways to tailor an acquisition's life cycle in these cases.

7. RELATED DOCUMENTS

General

1. Agency System Life Cycle Management Procedure: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

2. EPA IRM Policy Manual: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

3. EPA Order 2100.1, Accessible Electronic and Information Technology, January 2002: **http://intranet.epa.gov/rmpolicy/ads/orders/2100_1.pdf**

Systems Life Cycle

1. EPA Order 2195.1A4, Agency Network Security Policy, March 2001: **http://intranet.epa.gov/rmpolicy/ads/orders/2195.1A4.pdf**

2. OCFO Policy Announcement 01-03, May 23, 2001: **http://intranet.epa.gov/ocfo/policies/policy/pa01.htm**

3. OCFO Policy Announcement 01-10, September 28, 2001: **http://intranet.epa.gov/ocfo/policies/policy/pa01.htm**

4. OCFO Policy Announcement 05-01, December 15, 2004, "Accounting for Information Technology" **http://intranet.epa.gov/ocfo/policies/policy/pa05.htm**

Management Review and Approval

1. CIO Policy 06-001 (2120.3), Enterprise Architecture Policy, November 17, 2005: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

2. CIO Policy 06-003 (2100.3,) Information Technology Capital Planning and Investment Control (CPIC), December 15, 2005: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

3. CPIC Procedures for the OMB Exhibit 300, December 2004: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

4. Earned Value Management Procedures, Addendum to CPIC Procedures, December 2004: **http://intranet.epa.gov/oei/imitpolicy/policies.htm**

System Classification

1. NIST FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, **http://csrc.nist.gov/publications/fips/index.html**

2. NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," June 2004 **http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf**

3. OMB Circular A-11, (**http://www.whitehouse.gov/omb/circulars/index.html**)

- Section 52, Information on Financial Management

- Section 53, Revised, Information Technology and E-Government

4. OMB Circular A-127, Section 8, Revised, Financial Management Systems: **http://www.whitehouse.gov/omb/circulars/index.html**

5. OMB Circular A-130, Revised, Management of Federal Information Resources: **http://www.whitehouse.gov/omb/circulars/index.html**

6. OMB Memorandum 00-07, Incorporating and Funding Security and Information System Investments, February 28, 2000:
http://www.whitehouse.gov/omb/memoranda/2000.html

7. OMB Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 17, 2001:
http://www.whitehouse.gov/omb/memoranda/2002.html

System Life Cycle Management

1. EPA National Records Management Program (NRMP):
http://www.epa.gov/records/index.htm

2. NIST Special Publications for security guidance:
http://csrc.nist.gov/publications/nistpubs/

3. NIST Special Publication 800-64, Security Considerations in the Information System Development Cycle, October 2003:
http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

4. Policy and Program Requirements for the Mandatory Agency-wide Quality System, May 2000: **http://www.epa.gov/quality**

Roles and Responsibilities

1. Senior Information Officials (SIO) Policy (CIO Policy Transmittal 05- 001), July 2005
http://intranet.epa.gov/oei/imitpolicy/policies.htm

EPA Classification No.: 2100.5	CIO Approval Date: 4/7/06
CIO Transmittal No.: 06-009	Review Date: 4/09

8. ROLES AND RESPONSIBILITIES:

A. Chief Information Officer (CIO) is responsible for:

1. Approving the SLCM Policy

2. Ensuring Agency compliance with the SLCM Policy by providing guidance and tools to senior level managers for program oversight

3. Approving/disapproving waivers to the SCLM Policy

B. Assistant Administrators, Chief Financial Officer, General Counsel, Inspector General, Deputy Chief of Staff to the Administrator, Associate Administrators, and Regional Administrators and Laboratory Directors are responsible for:

Ensuring oversight and compliance with this Policy, and its supporting procedures, standards and guidance within their organizations

C. Chief Technology Officer (CTO) is responsible for:

1. Establishing and publishing procedures, technical operational directives and standards, and guidance supporting the Agency's SLCM Policy,

2. Approving the SLCM Procedure,

3. Reviewing and granting waivers from the SLCM Procedure for General Support Systems and Major Applications and Major Investments defined by the CPIC process

(For waivers from this Policy, please refer to the Chief Information Officer's Roles and Responsibilities above)

D. Director of OEI's Office of Technology Operations and Planning (OTOP) is responsible for:

1. Maintaining the SLCM Policy and SLCM Procedure

2. Monitoring compliance with this Policy through the IT Investment Management processes, specifically CPIC and EA, and security processes

E. Chief Architect is responsible for:

1. Leading the development, alignment and maintenance of the Agency's target Enterprise Architecture in conjunction with the SLCM Policy

2. Certifies that Solutions Architectures required for IT projects are compliant with the Enterprise Architecture

F. Director of the Office of Acquisition Management (OAM) is responsible for:

1. Ensuring requests for proposals and contracts incorporate and/or reference the SLCM Policy, as appropriate

G. Senior Information Officials (SIOs) are responsible for:

1. Ensuring the Quality and Information Council (QIC) is apprised of major SLCM issues within their office

2. Ensuring oversight and compliance with this SLCM Policy for systems within their Office

3. Reviewing, concurring and/or approving waivers to the SLCM Policy and SLCM Procedure for Non-Major systems (i.e., those NOT in the CPIC process)

4. Ensuring that the information technology utilized and managed by their organization supports its business needs and mission, and helps to achieve EPA's strategic goals

H. Information Management Officers (IMOs) are responsible for:

1. Reviewing and concurring on waiver requests to the SLCM Policy and the SLCM Procedure

2. Reviewing documents contained in SMP as appropriate

3. Supporting their SIOs to ensure compliance with this Policy

I. Information Security Officers (ISOs) are responsible for:

1. Ensuring that responsible program offices and individuals throughout the AA-ship or Regional Office are cognizant of security requirements and processes throughout a system's life cycle

J. System Sponsors are responsible for:

1. Authorizing, approving and ensuring adequate funding and resources during the life cycle of an information system

2. Appointing system owners and authorizing those individuals to initiate system development

K. System Owners are responsible for:

1. Monitoring compliance to the SLCM Policy

2. Concurring on waiver requests from the SLCM Policy and/or SLCM Procedure as applicable

3. Appointing System Managers

4. Coordinating SLCM development activities with those of the EPA IT Investment Management processes, specifically CPIC and EA processes

5. Ensuring compliance to Section 508 requirements during SLCM

6. Accounting for information system costs according to the cost accounting phases

defined in the EPA's cost accounting policy

L. System Managers are responsible for:

1. Providing day-to-day management of the system life cycle process and products within their program(s)

2. Ensuring that the system advances through the SLCM phases

3. Recommending and preparing written justification for waivers and including the request and decision for waivers as part of the SMP

4. Identifying, and keeping management apprised of, project issues and risks

M. Project Managers (PM) are responsible for:

1. Managing their project through its life cycle and ensuring compliance with this Policy. PMs must be qualified in accordance with Federal and Agency requirements for IT project management, and possess documented knowledge and skills as prescribed by the qualification guidance.

N. Privacy Act Officer is responsible for:

1. Ensuring that adequate safeguards against disclosure of information protected under the Privacy Act are incorporated into the system

O. Records Officers are responsible for:

1. Managing, filing and storing records related to a system's life cycle

9. DEFINITIONS

Application: The use of information resources (information and information technology) to satisfy a specific set of user requirements (OMB A-130, App. III). In particular, an application is usually considered to be the software component of a system. An application runs on, and may or may not be part of, a general support system.

The terms "application" and "information system" are sometimes used interchangeably although the latter has a broader definition.

Capital Planning and Investment Control (CPIC) process: The decision-making process for ensuring information technology investments which integrates strategic planning, budgeting, procurement, and the management of IT in support of Agency missions and business needs. The term comes from the Clinger-Cohen Act (CCA) of 1996 and generally is used in relationship to IT management issues.

Checkpoint: A specific calendar driven point during the system life cycle when the system owner assesses the progress of the SLCM process to ensure that the activities associated with this process are coordinated with and support the CPIC, EA and IT Security requirements.

Classification: EPA utilizes the Major Applications and General Support Systems classifications defined in OMB Circular A-130, Appendix III, and the Major Investment classification defined in the CPIC process. In addition, FIPS PUB 199 sets mandatory standards for categorizing Federal information systems. The use of FIPS PUB 199 in categorizing systems and information in combination with a risk assessment directly impacts the selection of security control requirements within the systems life cycle process. NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories" assists Federal agencies in categorizing information systems in relation to the mandatory standards in FIPS PUB 199.

Commercial Off-The-Shelf (COTS): A product or information system available in the commercial market place. COTS products are sold to the general public in the course of normal commercial business operations at prices based on established catalog or market prices (Federal Acquisition Regulations). COTS products are delivered with pre-established functionality, although some degree of customization is often possible.

Control Gates: Phase-driven go/no-go decision points where SLCM activities are reviewed to ensure that appropriate OMB and EPA requirements are observed. A system cannot proceed without a "go" decision by the appropriate senior manager for the specific control gate.

Contingency Planning: This planning is necessary to ensure the capability to perform an Agency function supported by an application in the event of failure of its automated support.

Enterprise Architecture (EA): A strategic information asset base which defines business mission needs, the information content necessary to operate the business, the information technologies necessary to support business operations, and the transitional processes necessary for implementing new technologies in response to changing business mission needs. Enterprise architecture includes baseline architecture, target

architecture and a sequencing plan.

General Support System: As defined by OMB Circular A-130, Appendix III, it is an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.

Government Off-The-Shelf (GOTS): A product developed by or for a government agency and that can be used by another government agency with the product's pre-established functionality and little or no customization.

Information System Projects: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, and disposition of information. The term can refer to an application, a system, a general support system, or the service components that make up a system.

IT Investment Management Review: A process for reviewing CPIC and EA IT investments. The process was developed using the requirements of the Clinger-Cohen Act, and guidance from the General Accounting Office and the Office of Management and Budget. A senior management IT investment review board may review project advancements from one SLCM phase to the next.

Major Application/System: As defined by OMB Circular A-130, Appendix III, an application or system that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Major Investment: For EPA's OMB budget reporting, all major IT investments must be reported on the Exhibit 53 and must submit a "Capital Asset Plan and Business Case," Exhibit 300. EPA uses the OMB's definition of a major investment, which can be found in the CPIC Procedures document.

Small Desktop Applications: Refers to end-user programs or application software that resides solely on a desktop or laptop. While it may be interconnected with other applications on the desktop/laptop (e.g. Microsoft Office Suite), they are not involved in controlling, integrating, or managing components of a system.

Solution Architecture: A Solution Architecture describes how an individual information management system, or information acquisition, will comply with the requirements of the Target Architecture, which is the set of products that portrays the future state of the Agency. A Solution Architecture is a comprehensive architectural response to a business problem. Solutions address all layers of Enterprise Architecture - strategy, business, data, applications and technology/security.

System Management Plan (SMP): A compilation of managerial documents required in the life of an information system. The required documentation varies by the classification of the system and changes over the life of system as it moves through the phases.

EPA Classification No.: 2100.5	CIO Approval Date: 4/7/06
CIO Transmittal No.: 06-009	Review Date: 4/09

10. WAIVERS

1. Waivers to the requirements of this Policy may be considered based on the requirements of the system and needs of the developing office. All waivers must be justified and documented (including all approvals and concurrences), as part of the System Management Plan.

2. Any waiver requests for Major Applications, General Support Systems and systems considered to be Major Investments in the CPIC process must include a signed concurrence by the System Owner and Senior Information Official (SIO). The Chief Information Officer will approve SLCM Policy waivers. The Chief Technology Officer will approve waivers from the SLCM Procedure or applicable standards.

3. The System Owner and the SIO approve waivers for any other (those not included in the CPIC process) applications and/or systems. Approved waivers are documented and added to the System Management Plan.

11. RELATED PROCEDURES AND GUIDELINES

Systems Life Cycle Management Procedure

12. MATERAL SUPERSEDED

This Policy supersedes the Interim Agency Systems Life Cycle Management Policy, Agency Directive 2100.4

13. ADDITIONAL INFORMATION

For questions about this Policy, please contact the Office of Environmental Information, Office of Technology Operations and Planning, Mission Investment Solutions Division at (202) 566-0330.

Linda A. Travers, Acting Assistant Administrator
and Chief Information Officer
Office of Environmental Information